Организация процесса выявления и реагирования на компьютерные инциденты и взаимодействия с НКЦКИ

Управление информационной безопасности

Комаров В.В.
19.11.2019

ДЕПАРТАМЕНТ
ИНФОРМАЦИОННЫХ
ТЕХНОЛОГИЙ
ГОРОДА МОСКВЫ

ДИТ

Регулирующие нормативно-правовые документы

РОССИЙСКАЯ ФЕДЕРАЦИЯ
ФЕДЕРАЛЬНЫЙ ЗАКОН

О безопасности критической информационной инфраструктуры Российской Федерации
№ 187 от 26.07.2017
Статья 5, 9

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ (ФСТЭК России)
ПРИКАЗ
_____ № _____
Москва

ТРЕБОВАНИЯ
По обеспечению безопасности значимых объектов КИИ РФ
№ 239 от 25.12.2017
Раздел 13, 22

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ПРИКАЗ
_____ № _____
Москва

ПОРЯДОК
информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов КИИ РФ
№ 282 от 19.07.2019

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ПРИКАЗ
_____ № _____
Москва

Перечень информации, предоставляемой в ГосСОПКА
№ 367 от 24.07.2018

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ПРИКАЗ
_____ № _____
Москва

ПОЛОЖЕНИЕ
о Национальном координационном центре по компьютерным инцидентам
№ 366 от 24.07.2018

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ПРИКАЗ
_____ № _____
Москва

ПОРЯДОК
обмена информацией о компьютерных инцидентах
№ 368 от 24.07.2018

ДИТ

03

11

Процесс выявления и реагирования на КИ субъектом КИИ

01
Выявление КИ

02
Предупреждение

03
Реагирование

04
Информирование НКЦКИ

05
Регистрация

ДИТ

04

Источники информации о компьютерном инциденте

11

Пользователи объекта КИИ (внутренние)

Служба техподдержки (внутренняя)

Техподдержка поставщика / оператора (внешняя)

НКЦКИ / ФСБ / ФСТЭК

СМИ

Пользователи систем, взаимодействующих с объектом КИИ (внешние)

ДИТ

05

Участники процесса

11

Ответственные сотрудники

Пользователи

Задачи ответственных сотрудников

Контроль и управление процессом

Выявление (обнаружение) КИ

Информирование коллег и руководства

Реагирование на КИ
Регистрация КИ

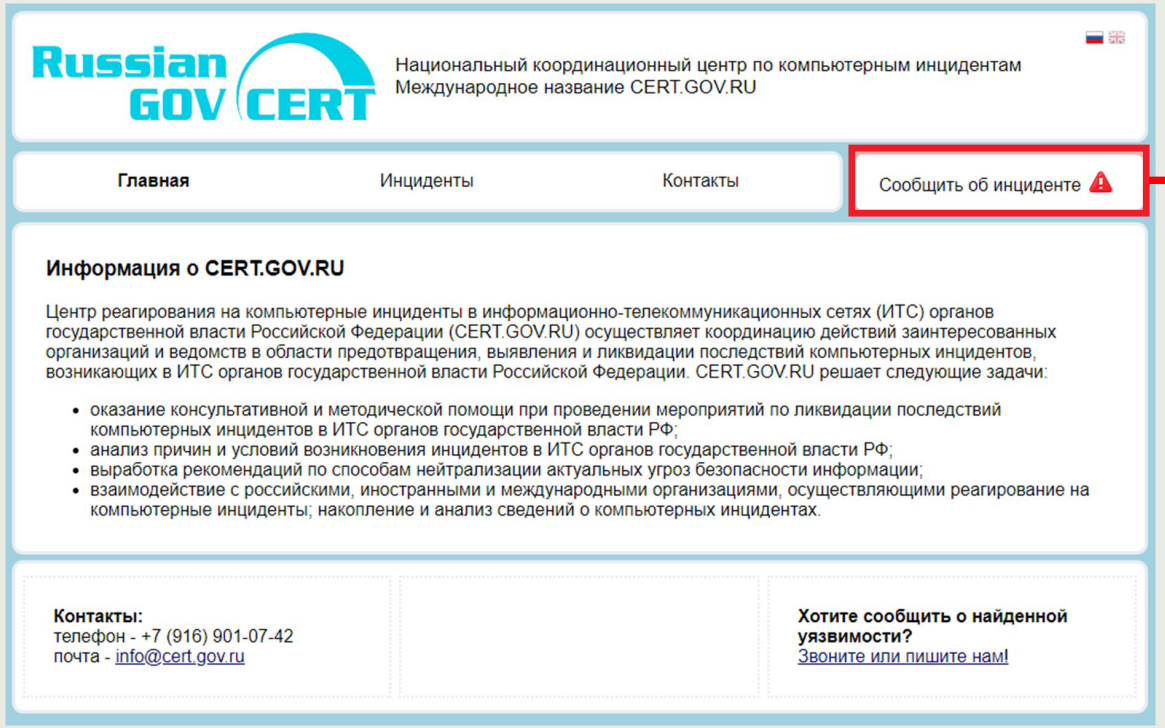
Взаимодействие с НКЦКИ

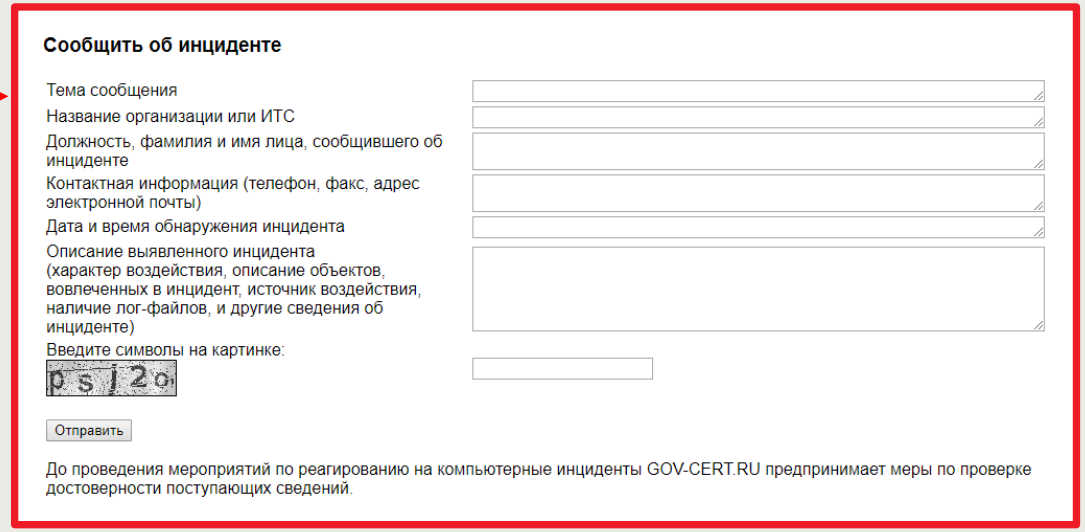
Сбор и подготовку информации о КИ

ДИТ

Каналы информирования НКЦКИ

› Сайт CERT.GOV.RU





› Телефон

+7 (916) 901-07-42

› Почта

incident@cert.gov.ru

ДИТ

07

11

Какую информацию передавать в НКЦКИ

Субъект КИИ с незрелой ИБ

Карточка регистрации компьютерного инцидента

Наименование объекта КИИ:	
Категория значимости объекта КИИ:	
Местонахождение объекта КИИ:	
Дата возникновения инцидента:	Время возникновения инцидента:
Регистрационный номер инцидента:	Связанные события/инциденты:
Контактные данные работника, обрабатывающего инцидент:	
ФИО: Организация: Контактные данные:	Адрес: Подразделение: e-mail:
Общее описание компьютерного инцидента:	
Что произошло: Как произошло: Почему произошло: Технические параметры инцидента: Последствия инцидента:	

ДИТ

08

11

Какую информацию передавать в НКЦКИ

Субъект КИИ со зрелой ИБ

Форма регистрации компьютерного инцидента

Учетный №:	Наименование объекта КИИ:
Категория значимости объекта КИИ:	Местонахождение объекта КИИ:
Взаимодействие с сетями электросвязи:	Дата и время заполнения:
Должность и ФИО лица, ответственного за регистрацию компьютерного инцидента:	
Основные сведения о компьютерном инциденте:	
Дата и время возникновения инцидента:	Нарушение конфиденциальности, целостности, доступности:
Нарушение конфиденциальности, целостности, доступности:	полное/частичное/ отсутствует
Описание инцидента (о функционировании объекта):	Класс инцидента (выбрать один):
Характеристика инцидента (кратко, тип инцидента, использованная уязвимость):	НСД к ИР/блокирование доступности элементов непреднамеренное нарушение:
Контактные данные работника, выявившего инцидент:	
ФИО: Организация: Контактные данные:	Адрес: Подразделение: e-mail:
Контактные данные работника, обрабатывающего инцидент:	
ФИО: Организация: Контактные данные:	Адрес: Подразделение: e-mail:
Дополнительные сведения:	
Выявленные уязвимости: Сведения о средстве/способе выявления КИ: Хронология принятых мер:	Результат принятых мер: Последствия инцидента (выбрать один вариант):
Технические сведения:	**Дополнительная информация:**

ДИТ

Контроль и учет компьютерных инцидентов

Журнал учета компьютерных инцидентов (КИ)												
№	Наимено-вание объекта КИИ	Категория значимос-ти ОКИИ	Местонахожде-ние объекта КИИ	Учетный № формы	Время и дата фиксирова-ния КИ	Класс КИ	Краткое описание КИ	Нанесенный ущерб	Время простоя (часов)	Оповещенные сотрудники организации (ФИО, должнось)	Дата и время оповещения НКЦКИ	Отметка об устранении последствий
1												
2												
3												
4												
5												
6												
7												

ДИТ

10

11

Разрабатываемые методические документы

(типовые)

- Приказ о назначении ответственных
- Должностные инструкции (инструкции для ответственных)
- Регламент выявления и реагирования компьютерных инцидентов
- План реагирования на компьютерные инциденты
- Регламент взаимодействия с НКЦКИ
- Форма карточки инцидента
- Журнал учета компьютерных инцидентов

Всегда на связи!

ДИТ

twitter.com/**ditmos**

vk.com/**ditmos**

www.mos.ru/**dit/**

ok.ru/**ditmos**

facebook.com/**ditmos**